

The Braunstone Life Community Newspaper

General Data Protection Regulations Policy

Policy prepared: May 2018
Approved by Board:
Policy Review: May 2020 unless the law changes beforehand.

The Braunstone Life Community Newspaper needs to gather and use certain information about individuals: these can include customers, suppliers, business contacts, volunteers and other people who we may need to contact or those who may need to contact us.

This policy describes how this personal data must be collected, handled and stored to comply with UK law and our own data protection standards.

The policy ensures that the Braunstone Life Community Newspaper

- Complies with data protection law and follows good practice
- Protects the rights of volunteers, customers and others
- Is open about how we store and process individuals' data
- Protects ourselves from the risk of a data breach

Data Protection Law

The Data Protection Act 1998 describes how organisations, including the Braunstone Life Community Newspaper must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that data must:

- 1 Be processed fairly and lawfully
- 2 Be obtained only for specific, lawful purposes
- 3 Be adequate, relevant and not excessive
- 4 Be accurate and kept up to date
- 5 Not be held for any longer than necessary
- 6 Processed in accordance with the rights of data subjects
- 7 Be protected in appropriate ways
- 8 Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

This policy applies to all Board members, volunteers, advertisers/customers, suppliers or people working on behalf of those suppliers, and those who have made enquiries about advertising or volunteering for the Braunstone Life Community Newspaper.

It applies to all data that the Braunstone Life Community Newspaper holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- or any other information relating to individuals.

Data Protection Risks

This policy helps to protect the Braunstone Life Community Newspaper from very real data security risks, including:

- Breaches of confidentiality, ie., information being given out inappropriately.
- Failing to offer choice, ie., all individuals should be free to choose how the company uses data relating to them.
- Reputational damage, ie., the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works (volunteers) for or with the Braunstone Life Community Newspaper has some responsibility for ensuring data is collected, stored and handled appropriately.

Everyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that the Braunstone Community Life Newspaper meets its legal obligations.
- The **Data Protection Officer, Roy Sherwin**, is responsible for
 - ~ Keeping the board updated about data protection responsibilities, risks and issues.
 - ~ Reviewing all data protection procedures and related policies, in line with the agreed schedule.

- ~ Arranging data protection training and advice for the people covered by this policy.
 - ~ Handling data protection questions from volunteers and anyone else covered by this policy.
 - ~ Dealing with requests from individuals to see the data held about them (subject access requests).
 - ~ Checking and approving any contracts or agreements with third parties.
 - ~ Addressing any data protection queries from journalists.
- The **IT Manager, Lin Burrows**, is responsible for:
 - ~ Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
 - ~ Performing regular checks and scans to ensure security hardware and software is functioning properly
 - ~ Evaluating and third-party services the company is considering using to store or process data, ie, cloud computing services.
 - The **Marketing Manager, Jacky Stamp**, is responsible for:
 - ~ Approving any data protection statements attached to communications such as emails and letters.
 - ~ Where necessary, working with other volunteers/staff to ensure marketing initiatives abide by data protection principles.

General volunteer/staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work, ie., Editor, Treasurer, Distribution Manager, Adverts Manager.
- Data **should not be shared informally**. When access to confidential information is required, volunteers can send a request to the Editor.
- Volunteers should keep all data secure by taking sensible precautions and following the guidelines below:
 - **Strong passwords** should be used and never shared.
 - Personal data should not be disclosed to unauthorised people, either within the company or externally.
 - Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
 - Volunteers should request help from the officers above, if they are unsure of any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions relating to storage should be directed to the officers above.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

When data is **stored electronically but has been printed out** for any reason:

- When not required, the paper/printouts should be stored in a locked cupboard/drawer.
- All printouts should not be left where they can be seen by unauthorised persons.
- Data printouts should be shredded and securely disposed of when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Data should be protected by strong passwords that are changed regularly and never shared.
- If data is **stored on removable media** (DVD/CD or External Hard Drive, etc.,) these should be kept locked away when not in use.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be sited in a secure location, away from normal office space.
- Data should be **backed up frequently**.
- **Unencrypted data** should **never be saved directly** to laptops or other mobile devices, tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of no value to the Braunstone Life Community Newspaper unless the company can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, volunteers should ensure the screens of the computer is locked when left unattended.
- Personal data should not be shared informally and should never be sent by email as this is not secure.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside the European Economic Area.

Data Accuracy

The law requires the Braunstone Life Community Newspaper to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all volunteers/staff who work with data to take reasonable steps to ensure data is accurate and as up to date as possible.

- Data will be held in as few places as necessary.
- Volunteers/staff should take every opportunity to ensure data is updated.
- The Braunstone Life Community Newspaper will make it easy for data subject to update their information.
- Data should be updated as inaccuracies are discovered. Inaccurate information should be deleted.

Subject Access Requests

All individuals who are the subject of personal data held by the Braunstone Life Community Newspaper are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a Subject Access Request. Subject Access Requests from individuals should be made by email to editor@braunstonelife.com

Individuals will be charged £10 per Subject Access Request - the relevant information will be provided within fifteen working days. The identity of anyone making a request will be verified before information is handed over.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, the Braunstone Life Community Newspaper will disclose requested data. However the Data Protection Officer will ensure the request is legitimate, seeking assistance from the board and the company's legal advisors where necessary.

Providing information

The Braunstone Life Community Newspaper aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights.

To this end, the company has a privacy statement, setting out how data relating to individuals is used by the company. This is available on request. A version of this statement is also available on the company's website.

